Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A validation protocol for determining authenticity of a printer consumable, said protocol including the steps of:

providing a printer containing a ~~trusted~~ first authentication chip and a printer consumable containing ~~an untrusted~~a second authentication chip;

generating a secret random number and calculating a signature for the secret random number using a signature function, in the ~~trusted~~ first chip, the ~~trusted~~ first chip having a random function to produce random numbers from a seed, and the function advances after each successful validation, so that the next random number is produced from a new seed;

encrypting the secret random number and the signature by a symmetric encryption function using a first key, in the ~~trusted~~ first chip;

passing the encrypted secret random number and signature from the ~~trusted~~ first chip to the ~~untrusted~~ second chip;

decrypting the encrypted secret random number and signature with a symmetric decryption function using the first key, in the ~~untrusted~~ second chip;

calculating a signature for the decrypted secret random number using the signature function, in the ~~untrusted~~ second chip;

comparing the signature calculated in the ~~untrusted~~ second chip with the signature decrypted, in the ~~untrusted~~ second chip;

in the event that the two signatures match, in the ~~untrusted~~ second chip, encrypting the decrypted secret random number by the symmetric encryption function using a second key and returning the encrypted secret random number to the ~~trusted~~ first chip;

calling a test function in the ~~trusted~~ first chip, the test function being called by the ~~trusted~~ first chip first receiving, a plural and random number of times, a first number, then receiving the encrypted secret random number from the ~~untrusted~~ second chip, the plural and random number of times being determined based on a clock signal, the test function including:

encrypting the secret random number by the symmetric encryption function using the second key, in the ~~trusted~~ first chip, to produce a second number;

comparing, up to said plural and random number of times, the second number with the first number, in the ~~trusted~~ first chip, the first number being selected such that the comparison should never return a match in the ~~trusted~~ first chip,

in the event that the current comparison with the first number returns a match, considering the ~~trusted~~ first chip to be invalid and terminating the protocol;

in the event that all of the comparisons with the first number return a mismatch, comparing the second number with the encrypted secret random number from the ~~untrusted~~ second chip, in the ~~trusted~~ first chip;

in the event that the comparison with the encrypted secret random number from the ~~untrusted~~ second chip returns a match, considering the ~~untrusted~~ second chip to be valid and authorizing use of the printer consumable; and

in the event that the comparison with the encrypted secret random number from the ~~untrusted~~ second chip returns a mismatch, considering the ~~untrusted~~ second chip to be invalid and denying use of the printer consumable.

2. (Currently Amended) The protocol according to claim 1, where the first and second keys are held in both the ~~trusted~~ first and ~~untrusted~~ second authentication chips, and are kept secret.

3. (Cancelled)

4. (Currently Amended) The protocol according to claim 1, where the symmetric decrypt function is held only in the ~~untrusted~~ second chip.

5. (Currently Amended) The protocol according to claim 1, where the signature function generates digital signatures of 160 bits.

6. (Cancelled)

7. (Currently Amended) The protocol according to claim 6, where the time taken to return an indication the second chip is invalid is the same for all bad inputs, and the time taken to return the secret random number encrypted with the second key is the same for all good inputs.

8. (Currently Amended) The protocol according to claim 1, where a test function is held only in the ~~trusted~~ first chip to advance the secret random number if the ~~untrusted~~ second chip is valid; otherwise it returns an indication the second chip is invalid.

9. (Currently Amended) The protocol according to claim 8, where the time taken to return an indication the second chip is invalid is the same for all bad inputs, and the time taken to return an indication the second chip is valid is the same for all good inputs.

10. (Original) The protocol according to claim 1, where it is used to determine the physical presence of a valid authentication chip.

11. (Currently Amended) A validation system for performing the method according to claim 1, where the system includes a printer containing a ~~trusted~~ first authentication chip and a printer consumable containing ~~an untrusted~~a second authentication chip; where the ~~trusted~~ first authentication chip includes a random number generator, a symmetric encryption function and two keys for the function, a signature function and a test function; and the ~~untrusted~~ second authentication chip includes a symmetric encryption and decryption function and two keys for these functions, a signature function, and a prove function to decrypt a secret random number and signature encrypted using the first key by the ~~trusted~~ first authentication chip, and to calculate another signature from the decrypted secret random number, for comparison with the decrypted signature, and in the event that the comparison is successful to encrypt the secret random number with the second key and send the encrypted secret random number back; the test function in the ~~trusted~~ first chip then operates to generate an encrypted version of the secret random number using the second key and to compare the encrypted secret random number with the received version to validate the ~~untrusted~~second chip, where the ~~trusted~~ first authentication chip contains a random function to produce random numbers from a seed, and the function advances after each successful validation, so that the next random number will be produced from a new seed.

12. (Currently Amended) A validation system according to claim 11, where the remainder of the system is software, hardware or a combination of both, but the ~~trusted~~ first chip is a physical authentication chip.

13. (Original) A validation system according to claim 11, where both chips have the same internal structure.

14. (Original) A validation system according to claim 11, where the first and second keys are kept secret.

15. (Cancelled)

16. (Original) A validation system according to claim 11, where the signature function generates digital signatures of 160 bits.

17. (Currently Amended) A validation system according to claim 11, where the prove function returns an indication the second chip is invalid for all bad inputs and the time taken to do this is the same for all bad inputs, and the time taken to return the secret random number encrypted with the second key is the same for all good inputs.

18. (Currently Amended) A validation system according to claim 11, where the test function advances the secret random number if the ~~untrusted~~ second chip is validated.

19. (Currently Amended) A validation system according to claim 11, where the time taken for the test function to return an indication the second chip not validated is the same for all bad inputs, and the time taken to return an indication that the second chip is validated is the same for all good inputs.

20. (Original) A validation system according to claim 11, where it is used to determine the physical presence of a valid authentication chip.